

UNITED STATES DISTRICT COURT

for the
Western District of Arkansas
Fayetteville Division

US DISTRICT COURT
WESTERN DISTRICT OF ARKANSAS
FILED

MAR 02 2020

DOUGLAS F. YOUNG, Clerk
By
Deputy Clerk

IN THE MATTER OF THE SEARCH OF INFORMATION
ASSOCIATED WITH WORLDEDGE@YAHOO.COM,
THAT IS STORED AT PREMISES CONTROLLED BY
OATH INC.

Case No.

5:20cm23

Filed Under Seal

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (*identify the person or describe property to be searched and give its location*):

See "Attachment A"

located in the Eastern District of Virginia, there is now concealed (*identify the person or describe the property to be seized*):

See "Attachment B"

The basis for the search under Fed. R. Crim. P. 41(c) is (*check one or more*):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

18 U.S.C. § 1343
18 U.S.C. § 1349
18 U.S.C. §§ 1956 and 1957

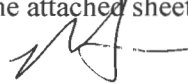
Offense Description

Wire Fraud
Conspiracy to Commit Wire Fraud
Money Laundering

The application is based on these facts:

☒ Continued on the attached sheet.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

Nathaniel Nantze, Special Agent,
Internal Revenue Service Criminal Investigation

Sworn to before me and signed in my presence.

Date: 3/2/2020



Judge's signature

City and state: Fayetteville, Arkansas

Erin L. Wiedemann, Chief United States Magistrate Judge

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF ARKANSAS

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH
WORLDEDGE@YAHOO.COM,
THAT IS STORED AT PREMISES
CONTROLLED BY OATH INC.

Filed Under Seal

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Nathaniel A. Nantze, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this Affidavit in support of an application for a search warrant for information associated with an account that is stored at premises controlled by Oath, Inc. d/b/a Verizon Media (formerly Yahoo! and AOL) (“Oath”), an email provider headquartered at 22000 AOL Way, Dulles, VA 20166. The information to be searched is described in the following paragraphs and in Attachment A. This Affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Oath to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I have been employed as a Special Agent with the Internal Revenue Service, Criminal Investigation, for over 17 years. I am currently assigned to the Fayetteville, Arkansas, post-of-duty in the Dallas field office. My responsibilities include the investigation of criminal violations of the internal revenue code (Title 26 United States Code), the Bank Secrecy Act (Title 31 United States Code), the Money Laundering Control Act (Title 18 United States Code), and

other related offenses. I have received training regarding income tax law and the investigation of financial crimes. I have conducted and participated in criminal investigations involving tax violations, money laundering, currency reporting violations, investment fraud, and other violations of the United States Code.

3. The facts in this Affidavit are based on (i) my training and experience; (ii) my review of documents and records, including documents provided by victim investors, and records received pursuant to grand jury subpoenas issued in this matter and search warrants for certain email accounts¹ issued by the Honorable Erin L. Wiedemann on April 29, 2019 in case number 5:19-cm-50 (W.D. Ark.), and on September 25, 2019, in case number 19-cm-105 (W.D. Ark.), pursuant to 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A); (iii) information obtained from other law enforcement authorities involved in the investigation, including the Federal Bureau of Investigation; (iv) information obtained from representatives of the victim investors; (v) the sworn testimony of Brian Brittsan, John Nock, Stanley Goldberg, and investors in the Brittingham Group provided during arbitration proceedings; (vi) interviews of victims of the scheme; (vii) information obtained from Google in response to a court order issued by the Honorable Erin L. Wiedemann pursuant to 18 U.S.C. § 2703(d) for certain account information since January 1, 2015 in case number 5:19-cm-19 (W.D. Ark.); (viii) information obtained from an interview of Brian Brittsan on September 22, 2019.

¹ On April 29, 2019, the Court issued search warrants on accounts belonging to co-conspirators of the scheme. The Court issued a search warrant for the account of bbrittsan@ljnets.com, which is stored at Network Solutions, LLC. The Court also issued a search warrant on eight account Google, LLC: brittinghamgroup@gmail.com; nockholdings@gmail.com; alex.sjl2015@gmail.com; asialotusinvestments@gmail.com; fdejacma@gmail.com; arthurmerson54@gmail.com; flower.louis@gmail.com; michaelferlazzo@gmail.com. In addition, on September 25, 2019, the Court issued a search warrant on bbrittsan@gmail.com, which is stored at Google, LLC.

4. This Affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

5. Based on my training and experience and the facts as set forth in this Affidavit, there is probable cause to believe that violations of 18 U.S.C. § 1343 (wire fraud), 18 U.S.C. § 1349 (conspiracy to commit wire fraud and mail fraud), and 18 U.S.C. §§ 1956 and 1957 (money laundering) have been committed by BRIAN BRITTSAN, JOHN NOCK, KEVIN GRIFFITH, ALEX ITUMA, STANLEY GOLDBERG, and others known and unknown. There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband, and/or fruits of these crimes further described in Attachment B.

6. The investigation to date reveals that the subjects have engaged in an investment fraud scheme in which they obtained millions of dollars in investments through false and misleading representations. To date, the victim investors have not realized any profits from their investment, nor have they received the principal in return.

JURISDICTION

7. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

8. The United States is investigating a scheme in which JOHN C. NOCK (“NOCK”), BRIAN D. BRITTSAN (“BRITTSAN”), KEVIN R. GRIFFITH (“GRIFFITH”), ALEXANDER ITUMA (“ITUMA”) and other co-conspirators solicited investments in entities they controlled, including the Brittingham Group, LLC (“Brittingham Group”), through false or misleading

representations. As further described below, GRIFFITH used the email account to be searched, worldedge@yahoo.com (the “Subject Account”), to further the scheme.

9. NOCK resides at XXXX N. Forest Heights, Fayetteville, AR, which is within the Western District of Arkansas. NOCK formed the Brittingham Group in 2010 and has solicited investments on behalf of the Brittingham Group since at least 2013. My investigation has revealed that CHARLES T. NOCK (“CHARLES NOCK”) is NOCK’s father and has provided accounting services to the Brittingham Group. CHARLES NOCK resides at XXXXX Meandering Way, Fort Smith, AR 72903.

10. As further described herein, BRITTSAN solicited investments on behalf of the Brittingham Group from a variety of investors. ITUMA and GRIFFITH are directors and beneficial owners of two entities that received much of the investment funds solicited on behalf of the Brittingham Group. BRITTSAN resides in San Marcos, CA, GRIFFITH resides in Provo, UT, and ITUMA resides in Lehi, UT.

11. I have reviewed a notarized affirmation of NOCK, dated June 5, 2018, in which NOCK wrote that GRIFFITH was the “director of the Asian operation” of the Brittingham Group and that ITUMA was a director of the Brittingham Group. I have also reviewed an email dated October 10, 2014 from NOCK, copying GRIFFITH using the Subject Account, in which NOCK identifies himself as Chairman of the Brittingham Group and identifies Griffith as the CEO of the Brittingham Group and states that GRIFFITH’s email is the Subject Account.

12. The Brittingham Group is a limited liability company formed by NOCK in the State of Arkansas on December 7, 2010. It has a registered office address of P.O. Box XXX, Fayetteville, AR 72702, and the registered agent is CHARLES NOCK, XXXXX Meandering Way, Fort Smith, AR 72903, both of which are within the Western District of Arkansas. The

Brittingham Group has maintained a bank account with a number ending 6836 at Bank of America since January 30, 2013. NOCK and CHARLES NOCK are the signatories on the account. The mailing address provided to Bank of America for the Brittingham Group is XXXX N. Forest Heights, Fayetteville, AR 72703-1864.

13. The investigation has revealed that NOCK, BRITTSAN, GRIFFITH, ITUMA and others solicited investment proceeds for entities they controlled, including the Brittingham Group, through false or misleading representations. Based in part on those misrepresentations, NOCK, BRITTSAN, and their co-conspirators obtained at least \$16,329,420 in investments from several individuals and entities. Approximately \$15,500,000 of those investments were transferred by the victim investors to accounts at banks located in Hong Kong. While the scheme is believed to be ongoing, the majority of the investments were made between in or about June 2015 and in or about January 2016. To date, the victim investors have not realized any profits from their investment, nor have they received the principal in return.

14. According to an interview of L.G. and documents provided by L.G., in approximately November 2013, NOCK told L.G. about a business NOCK was starting called the Brittingham Group. NOCK stated the business was going to make millions of dollars, but he needed money up front to pay for personal expenses until the business was generating revenue. NOCK asked to borrow \$25,000 from L.G. for a period of six months. L.G. agreed to make the loan to NOCK and prepared an Investment Agreement for NOCK to execute. NOCK provided L.G. with documentation describing the type of business deals the business would be conducting.

15. NOCK approached L.G. in May 2014 about borrowing an additional \$5,000 per month until the Brittingham Group completed its first transaction. L.G. agreed to loan the additional money to NOCK and prepared a new Investment Agreement that stated L.G. would

receive 5% of the revenue generated by the Brittingham Group. NOCK forwarded emails to L.G. that included documents detailing the status of the Brittingham Group's business deals in an effort to justify receiving the \$5,000 monthly payments. As described below, at least some of those documents are believed to be fraudulent. These documents may have been sent to L.G. in order to lull L.G. into believing that his loan was safe and secure, and induce L.G. into making further loans to the Brittingham Group. L.G. loaned NOCK a total of \$107,000 between November 2013 and January 2015, but to date has not received any money in return from NOCK.

16. Northwind Financial Corporation ("Northwind") and Bankers Capital, LLC ("Bankers Capital") are U.S.-based companies that assist clients in securing funding for various development projects. According to sworn testimony of J.S., a representative of Northwind, in June 2015, BRITTSAN and NOCK approached Northwind and Bankers Capital and represented that they, through the Brittingham Group and other entities under their control, could provide investment banking services that could assist Northwind and Bankers Capital's clients. NOCK and BRITTSAN made several misrepresentations to solicit funds from clients of Northwind and Bankers Capital, including Tierra Verde Escape, LLC ("Tierra Verde Escape"), TOW Development, LLC ("TOW Development"), and AMI Investment Holdings, LLC ("AMI Investment"). For instance, NOCK represented that he had extensive knowledge and experience in the types of credit enhancement transactions they were offering to investors. BRITTSAN and NOCK also claimed they had a current company office physically located at 14 Wall Street in New York, New York, an exclusive bank investment program through HSBC Bank, and established credit line facilities with and through Hong Kong companies Smart Jobs Limited, Gold Express Holdings Limited, and Rich Step Group Holdings Limited. NOCK, BRITTSAN, and the Brittingham Group promised significant returns to the investors – typically 100% of the principal

amount per week – that would be paid as quickly as 20 days from receipt of funds and each week thereafter. The Memorandums of Understanding between the Brittingham Group and each victim state that their proceeds would go towards the initial expenses related to developing structured finance programs and private investments arranged by the Brittingham Group. Based on the investigation to date, all of those representations are believed to be false.

17. Based in part on those and other representations, Tierra Verde Escape, TOW Development, and AMI Investment wired a total of \$150,000 directly to the Brittingham Group's Bank of America account. Additionally, between on or about July 17, 2015 and on or about September 15, 2015, the investors wired \$1,499,970 to HSBC Bank, Hong Kong, at the direction of NOCK and BRITTSAN. The HSBC accounts to which the victims wired the money were in the name of Smart Jobs Limited, account number ending 9838, and Gold Express Holding Limited, account number ending 4838. According to information received from a confidential source, JOE NIP ("NIP") was identified as a director of Smart Jobs Limited and Gold Express Holdings, Limited. ITUMA was identified as a director and beneficial owner of Smart Jobs Limited. ITUMA was identified as the beneficial owner of Gold Express Holdings Limited, and GRIFFITH was identified as the director of Gold Express Holdings Limited. To date, Tierra Verde Escape, TOW Development and AMI Investment have not received any money in return from their investment, nor have they received any documentation to confirm that the Brittingham Group ever invested their funds as promised.

18. BRITTSAN and NOCK also solicited investments from WIDEHA-UK LTD ("WIDEHA"), which is a Private Limited Company with a registered office address located in the United Kingdom. WIDEHA was formed by J.W., E.H. and J.P.D. on or about October 19, 2015, for the investment opportunity with the Brittingham Group. According to a written summary of

events prepared by counsel for WIDEHA, E.H. first spoke to ARTHUR MERSON about investing with the Brittingham Group. Based on the investigation to date, MERSON referred BRITTSAN to potential investors in the scheme. MERSON told E.H. that he had worked for BRITTSAN at the Brittingham Group for several years and that BRITTSAN and NOCK were “the best thing that ever happened.” To solicit funds from WIDEHA, beginning in or about November 2015, BRITTSAN and NOCK offered to provide a high yield structured financing contract through a proprietary managed buy/sell program. According to victim statements and review of email correspondence provided by the victims, BRITTSAN and NOCK offered a bullet trade – which is the act of buying a put option² where the value of the underlying asset is lower than the strike price and allows the buyer to capitalize on a downward-moving, or “bear” market – that they claimed provided historic returns averaging 100% per week during the trading period. BRITTSAN and NOCK stated that this would be followed by another bullet trade for the same amount to be completed before the Christmas holiday. WIDEHA’s funds were to be transferred to the Brittingham Group’s wholly-owned account at HSBC in the name of Smart Jobs Limited, for which GRIFFITH was the sole signatory. Upon receipt of the funds, BRITTSAN and NOCK represented that the Brittingham Group would utilize a short term transaction that would provide profit distributions within two weeks followed by subsequent short term trades with profit distributions at the end of each transaction. BRITTSAN and NOCK represented that the return of the principal would occur at the end of the trading period. The transaction would last for a trading period not to exceed twenty weeks unless agreed to by the parties. BRITTSAN and NOCK

² A put option is an option contract giving the owner the right, but not the obligation, to sell a specified amount of an underlying security at a specified price within a specified time frame.

represented that the transaction was estimated to produce profits averaging 85% during the first two weeks and would continue as agreed to by the parties.

19. In reliance upon these representations, on or about December 8, 2015, WIDEHA executed the Strategic Agreement with the Brittingham Group and transferred €10,000,000 to Hang Seng Bank Limited, Hong Kong (“Hang Sang”), account number ending 4883, in the name of Wealth Mark International Investment Limited (“Wealth Mark”). According to J.W., Wealth Mark is a company where the trades were to supposedly take place and is wholly owned by the Brittingham Group. According to an email dated December 8, 2015, BRITTSAN wrote to E.H., “As discussed I have revised the Agreement to change the Transaction Account to one of our holding Accounts; Wealth Mark International Investments LTD. at Hang Seng Bank Hong Kong. This is a pristine account that we currently acquired and your funds will not be comingled with any of our other transaction funds. We will provide full transparency of all account activity and look forward to the partnership.” WIDEHA was scheduled to start receiving profits within two weeks after investing its funds. On December 30, 2015, BRITTSAN represented in an email to J.W. and E.H. that the Hang Seng depository account number ending 4883 had a balance of 86,815,390.01 Hong Kong dollars – equivalent roughly to \$11,200,902 USD – as of December 23, 2015. Based on victim statements and email correspondence provided by the victims, NOCK and BRITTSAN continued to misrepresent via email, letters, and telephone that the €10,000,000 investment had been safely invested with Asia Lotus Investment Limited, Hong Kong, and that the Brittingham Group’s Hong Kong partner, GRIFFITH, was handling the trade. To date, WIDEHA has not received any money in return from its investment or confirmation that the Brittingham Group ever invested its funds as promised.

20. Based on my review of records and interviews of BRITTSAN and victim-investors S.C. and C.C., the Brittingham Group also obtained investments from four additional investors: S.C., C.C., C.A., and D.L. S.C. invested approximately \$150,000, C.C. invested approximately \$150,000, C.A. invested approximately \$230,000, and, according to BRITTSAN, D.L. invested \$2 million with the Brittingham Group.

21. In October 2017, Brian McCormick pleaded guilty to two counts of wire fraud in the United States District Court for the District of Maryland, in connection with his participation in a fraudulent scheme related to the Brittingham Group. According to the statement of facts admitted by the defendant and filed with the court, after communicating with NOCK and BRITTSAN, McCormick solicited investments into the Brittingham Group and misrepresented that he had personally invested his own funds in the Brittingham Group. McCormick first solicited investments into the Brittingham Group from Asset Depot Limited, which is an entity with a Registered Office located at Suite 2201, 22/F, Wing on House, 71 Des Voeux Road Central, Central, Hong Kong. On September 10, 2015, and September 16, 2015, Asset Depot Limited wired a total of €1,050,000 to HSBC Bank account number ending 4838, in the name of Gold Express Holdings. McCormick also solicited investments into the Brittingham Group from an individual, R.T., who wired €1,000,000 to HSBC Bank account number ending 9838, in the name of Smart Jobs Limited. In addition, McCormick solicited investments into the Brittingham Group from Peak Performance, an entity with a registered office located at Haywood House, Dumfries Place, Cardiff, CF10 3GA, United Kingdom. On January 13, 2016, Peak Performance wired €1,025,000 to HSBC Bank account number ending 9838, in the name of the Smart Jobs Limited. The Gold Express Holdings and Smart Jobs Limited accounts at HSBC Bank are the same bank accounts to which BRITTSAN and NOCK directed Tierra Verde Escape, TOW Development, and

AMI Investment to transfer some of their investments in the Brittingham Group. In sum, McCormick has pleaded guilty to fraudulently obtaining over €3 million in investments into the Brittingham Group that are apart from the \$16.1 million in investments previously described. The Brittingham Group has not repaid any investor and has not paid out any profits.

22. On September 22, 2019, IRS Special Agent Tim Arsenault and I interviewed BRITTSAN in San Marcos, California. After informing BRITTSAN of our identity as federal agents, BRITTSAN voluntarily agreed to answer our questions. During that interview, among other statements, BRITTSAN stated that he was involved with NOCK as a Director of the Brittingham Group. He stated that he first met NOCK in August 2013, and that they received funds for the first time from investors in 2015. BRITTSAN said that his role was to find investors and communicate updates and other information to investors, and NOCK's role was to find and manage investment products for the investors that Brittsan recruited. BRITTSAN also stated that he received updates from NOCK and other individuals via email, which BRITTSAN then communicated to investors. When speaking of the investment products that he was selling to investors, including standby letters of credit (SBLCs), bank guarantees, and medium term notes, BRITTSAN admitted that it was a "99.9% BS industry." BRITTSAN acknowledged that, since he has been involved with NOCK and the Brittingham Group, no investment has ever been paid out to the investors. BRITTSAN also stated that he has only met NOCK in person on one occasion, and that he continues to have regular communication with NOCK via email and phone.

23. Based on my review of the evidence obtained to date, GRIFFITH has used the Subject Account in furtherance of this fraudulent scheme.

24. I have reviewed emails from the Subject Account in which GRIFFITH communicated with co-conspirators in the scheme regarding purported financial transactions, the

movement of victim-investor funds, and documents designed to lull the victim investors into believing their funds were safe and that they would soon receive proceeds from their investments.

25. For instance, I have reviewed an email chain dated September 17, 2015, from NOCK to GRIFFITH at the Subject Account. Nock forwarded an email to the Subject Account and wrote, "He must have gotten this from SG ...". The original email that NOCK forwarded to GRIFFITH was from an individual that wrote, "John[,] Stop sending fake shit to my account I will report you and your ass . I'm fed up of the crap". The email included an attachment that purported to be a bank record documenting a standby letter of credit in the amount of \$4,800,000,000.00 from the Central Bank of Brazil. Based on my review of other records in this case that refer to STANLEY GOLDBERG using his initials, I submit that Nock was referring to co-conspirator STANLEY GOLDBERG in his email to GRIFFITH.

26. I have also reviewed an email dated July 22, 2014, from GRIFFITH, using the Subject Account, to NOCK. GRIFFITH wrote, "Please find the enclosed Scanned Copy of DTC Euro Clear Screen Message of HSBC USA's Bank Draft in the amount value of USD 2,639,500,000,000.00 (Two Trillion Six Hundred Thirty Nine Billion and Five Hundred Million Only) in favour of Centennial Energy (Thailand) Company Limited in order for your reference and submit to Mr. Ding for HSBC HK'S due diligence and KYC as required." GRIFFITH included a copy of a purported HSBC bank message referencing a "BANK DRAFT GUARANTEED" in the amount of \$2,639,500,000,000.00. NOCK then forwarded GRIFFITH's email, including the attachment, to two individuals and wrote, "Please look at the following Bloomberg screenshot. We have been presented this asset for possible control/management. It is in HSBC NY. We (or anyone we need) can be made the beneficiary. We will need some DD and

good intelligence to consider it.” Based on the total purported amount of the bank draft, I submit that GRIFFITH sent his co-conspirator a falsified bank record.

27. I have also reviewed an email chain dated October 20, 2015 from GRIFFITH, using the Subject Account, to ITUMA. GRIFFITH wrote to ITUMA, “John just called and asked for you to give him a letter regarding the 250K transfer and other subsequent transfers that you sent to South Africa... He asked that you explain and confirm the correct account name that the transfer was intended to be sent to. He wants you to state that you authorized all of these transfers and that you inadvertently left off the Proper Account Name on the 250K transfer, but that this letter confirms that the proper account name is fully authorized by you to receive this wire transfer and that you apologize for the confusion in not submitting the Correct Account Name on the 250K wire transfer. He needs you to also reference the other transfers you made and authorize all of these funds to be accepted by the receiving bank in South Africa... They have not been able to receive the 250K as a credit to the account because they are not sure you authorize this wire to the proper account name, since it was incorrectly filled out on your online wire transfer. Please prepare the above referenced letter, sign it and send to both me and John... They are saying if this money does not credit to the account then we will be short the required amount and they cannot hold our slot open on this transaction any longer”. That same day, ITUMA responded to the Subject Account and to NOCK and wrote, “KEV I HOPE THIS WORKS.” ITUMA attached a letter that stated, in part, “I, Alexander Ituma, the CEO of SMART JOBS LIMITED, AND SOLE SHARE HOLDER, and the account signatory, writing this letter to you in order to give full authority to immediately credit and deposit the amount of \$250,000.00 USD to RUBICOM PTY LTD TRADING AS CIRCLE HEALTHCARE, made on 16th OCT 2015.” Based on my review of records and interviews in this investigation, I know that on or about July 3, 2018, BRITTSAN

induced S.C. into investing \$150,000 in Circle Healthcare, which is the same entity referenced in the above-described email to GRIFFITH. To date, S.C. has not received any return on his investment.

28. I have also reviewed an email dated October 23, 2015, from GRIFFITH using the Subject Account to NIP and ITUMA. GRIFFITH wrote, “PLEASE SET UP WIRE TRANSFER FROM SMART JOBS LIMITED BANK ACCOUNT WITH VALUE DATE OF MONDAY 26 OCTOBER 2015. WE MUST GET A COPY OF THIS WIRE ONCE IT IS ENTERED WITH HSBC!! AMOUNT OF WIRE TRANSFER IS USD 2,050,000 - VALUE DATE MONDAY 26 OCTOBER 2015 MUST SHOW bank stamped and signed load copy PROVING THAT THIS WIRE TRANSFER HAS BEEN LOADED IN THE HSBC WIRE SYSTEM TODAY (FRIDAY 23 OCTOBER 2015) WITH OFFICIAL HSBC STAMP, SHOWING WIRE IS PROPERLY ORDERED AND INSTRUCTED TO BE SENT FROM SMART JOBS LIMITED TO THE BANK COORDINATES SHOWN BELOW”. GRIFFITH then specified the account details for the wire documentation for an account in the name of Rubicom PTY Limited Trading as Circle Health Care. Based on my review of bank records, on October 27, 2015, \$2,050,000.00 was sent from the Smart Jobs Limited account at HSBC – which had received some of the victim-investor funds – to account number ending 9570 at Firststrand Bank in the name of Rubicom PTY Limited Trading as Circle Health Care.

29. I have also reviewed an email chain dated February 17, 2016, from ITUMA to NOCK and GRIFFITH at the Subject Account. ITUMA forwarded to GRIFFITH and NOCK an email from NIP with the subject line, “Hang Seng Bank (Wealth Mark),” in which NIP wrote to ITUMA, “Important! We should not wire out any funds from HANG SENG BANK for at least 3 weeks from now for cool of [sic] period because HANG SENG BANK would think that we are

just using them to hold money and transfers no business with them, and if we don't, they will have it reported to HKMA and the funds will be frozen. Please inform your partners for this information." When ITUMA forwarded that email to GRIFFITH and NOCK, he wrote, "Am sure we can handle to wait till March 8th around that time to cool off things with Hang Seng, we don't need to give them any reason to even think they can report to HKMA. I personally know people this has happened to is not fun."

30. I have also reviewed an email dated March 29, 2016, from GRIFFITH using the Subject Account to another co-conspirator, WILLAH JOSEPH MUDOLO. GRIFFITH wrote, "Please see a simple draft of an email that will help the Client feel very happy about getting this wire transfer done for the 200+ Million to the London Bank Coordinates you provided me... If this can be placed on your letterhead with your signature and simply emailed to: brittinghamgroup@gmail.com with cc (copy) to worldedge@yahoo.com that would be great!!" GRIFFITH included draft language, to be signed by MUDOLO, which stated, "This letter confirms our readiness to receive your cash wire funds directly into our platform account for the purpose of executing the 'investment program' described by terms and conditions provided to you by The Brittingham Goup ('TBG'). Your funds will be secure and safe at all times and will not be placed at risk. We execute very large transactions on a regular basis and have been completing successful 'investment programs' for some of the strongest Governments and Investors from many locations around the world. We look forward to providing this service on your behalf and with coordination of our trusted associates at 'TBG'. We are prepared to proceed immediately upon receipt of your funds and look forward to our successful business together."

31. Based on my review of records, MUDOLO is the president of ADF Estates (Pty) Limited ("ADF Estates), which sent money to Smart Jobs USA LLC, which then sent money to a

bank account controlled by GRIFFITH. On May 31, 2016 and June 7, 2016, two transfers in the amounts of \$800,000.00 and \$500,000.00, respectively, were sent from DBS Bank Hong Kong account number ending 3050, in the name of ADF Estates, to Wells Fargo Bank account number ending 4536, in the name of Smart Jobs USA LLC. On June 1, 2016, and June 13, 2016, two wire transfers in the amounts of \$660,000.00 and \$500,000.00, respectively, were sent from Wells Fargo Bank account number ending 4536, in the name of Smart Jobs USA LLC, to Zions Bank account number ending 4025, in the name of the Valona Group Corporation. Griffith has sole signature authority on that Zions Bank account. Certified records obtained from the Utah Secretary of State identify Griffith as the President of the Valona Group Corporation and Ituma as a Director of the Valona Group Corporation.

32. I have also reviewed emails in which GRIFFITH used the Subject Account as early as October 2013 related to his work with NOCK and potential investors. For instance, on October 9, 2013, NOCK sent an email to an individual, copying GRIFFITH using the Subject Account, in which NOCK referenced assets in Brazil for restructuring and provided contact information for NOCK and GRIFFITH.

33. On September 23, 2019, the government formally requested, pursuant to 18 U.S.C. § 2703(f), that Oath preserve all stored communications, records, and other evidence currently relating to the Subject Account pending further legal process. On September 23, 2019, Oath confirmed receipt of that request with Oath reference number 426773. On December 16, 2019, the government sent a renewed request, pursuant to 18 U.S.C. § 2703(f), that Oath preserve all stored communications, records, and other evidence currently relating to the Subject Account pending further legal process. On December 16, 2019, Oath confirmed receipt of that request with Oath reference number 435075. In general, an email that is sent to an Oath subscriber is stored in

the subscriber's "mail box" on Oath servers until the subscriber deletes the email. If the subscriber does not delete the message, the message can remain on Oath servers indefinitely. Even if the subscriber deletes the email, it may continue to be available on Oath's servers for a certain period of time.

BACKGROUND CONCERNING EMAIL

34. In my training and experience, I have learned that Oath provides a variety of on-line services, including electronic mail ("email") access, to the public. Oath allows subscribers to obtain email accounts at the domain name @yahoo.com, like the email account listed in Attachment A. Subscribers obtain an account by registering with Oath. During the registration process, Oath asks subscribers to provide basic personal information. Therefore, the computers of Oath are likely to contain stored electronic communications (including retrieved and unretrieved email for Oath subscribers) and information concerning subscribers and their use of Oath services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

35. An Oath subscriber can also store with the provider files in addition to emails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to emails), and other files, on servers maintained and/or owned by Oath. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and files.

36. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such

information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

37. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (*i.e.*, session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

38. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a

result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

39. As explained herein, information stored in connection with an email account may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the IP addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculcate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (*e.g.*, location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime

(e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement).

CONCLUSION

40. Based on the forgoing, I request that the Court issue the proposed search warrant. Because the warrant will be served on Oath, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

REQUEST FOR SEALING

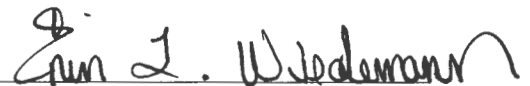
41. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee/continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

Respectfully submitted,



Nathaniel A. Nantze, Special Agent
Internal Revenue Service Criminal
Investigation Division

Subscribed and sworn to before me on this 2nd day of March, 2020.



Honorable Erin L. Wiedemann
Chief United States Magistrate Judge

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with worldedge@yahoo.com that is stored at premises owned, maintained, controlled, or operated by Oath, a company headquartered at 22000 AOL Way, Dulles, VA 20166.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Oath, Inc. (the “Provider”)

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on September 23, 2019, and December 16, 2019, 2019, the Provider is required to disclose within 14 days of this search and seizure warrant the following information to the government for each account or identifier listed in Attachment A:

a. The contents of all emails associated with the account from August 1, 2013 to present, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. The types of service utilized;

d. All records or other information stored by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files; and

e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken. The Provider is hereby ordered to disclose the above information to the government within 14 days of service of this warrant.

II. Information to be seized by the Government

All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of violations of 18 U.S.C. § 1343 (wire fraud), 18 U.S.C. § 1341 (mail fraud), 18 U.S.C. § 1349 (conspiracy to commit wire fraud and mail fraud), and 18 U.S.C. §§ 1956 and 1957 (money laundering), those violations involving JOHN NOCK, BRIAN BRITTSAN, ALEX ITUMA, KEVIN GRIFFITH, and others and occurring after August 1, 2013, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- (a) Investment in or work related to the Brittingham Group, LLC, Smart Jobs Limited, Gold Express Holdings, Wealth Mark International Investment, ADF Estates (Pty) Limited, Smart Jobs USA, Valona Group and SJL, LLC;
- (b) Communications between John C. Nock, Charles T. Nock, Brian Brittsan, Kevin Griffith, Alexander Ituma, Stanley Goldberg, Joe Nip, Frederick De Jacma, Arthur Merson, Michael Ferlazzo and/or Louis Flower;
- (c) Solicitation of investor funds;
- (d) Preparatory steps taken in furtherance of the scheme;
- (e) Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;

- (f) Evidence indicating the email account owner's state of mind, or the state of mind of co-conspirators, as it relates to the crime under investigation;
- (g) Evidence of additional co-conspirators or participants in the scheme;
- (h) Evidence of concealment of the scheme;
- (i) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

ADDENDUM TO ATTACHMENT B

With respect to law enforcement's review of the seized material from the Subject Account, law enforcement (i.e., the federal agents and prosecutors working on this investigation and prosecution), along with other government officials and contractors whom law enforcement deems necessary to assist in the review of the Subject Account (collectively, the "Review Team") are hereby authorized to review, in the first instance, the email account and the information and materials contained in it, as set forth in this Attachment B.

If law enforcement determines that all, or some, or a portion of the information or materials in the Subject Account contain or may contain information or material subject to a claim of attorney-client privilege or work-product protection (the "Potentially Privileged Materials"), the Review Team is hereby ordered to: (1) immediately cease its review of the specific Potentially Privileged Materials at issue; (2) segregate the specific Potentially Privileged Materials at issue; and (3) take appropriate steps to safeguard the specific Potentially Privileged Materials at issue.

Nothing in this Addendum shall be construed to require law enforcement to cease or suspend the Review Team's review of the Subject Account upon discovery of the existence of Potentially Privileged Materials in the Subject Account.